تخلص من أي فيروس

دون فورمات

دليلك للقضاء على أي فيروس كان أصاب جهازك حتى لو كان Tazebama. و صيانة حاسبك مما أفزدته الفيروسات... كأنك قمت بعملية فورمات لكنك إحتفظت بملفاتك وربحت الوقت...

حمدة العيساوي

أوت 2009

الحل الجذري للتخلص من أي دون فورم فيروس دون فورمات

<u>تمهيد:</u>

بين يديكم الان طريقة عملية للتتخلص من أي فيروس كان دون الحاجة إلى فرمتة الحاسوب وإعادة تنصيب النظام.

يلجئ الكثيرون لعملية فرمطة الحاسوب نظرى ليأسهم في محاربة الفيروس أو الدودة التي أصابة جهازهم من خلال برامج مكافحة الفيروسات وطرق أخرى عبر التعديل على الريجيتر وغيرها.

اليوم أقدم لكم هذه الطريقة المجربة شخصيا على عدة أنواع من الفيروسات والديدان في مجموعة مختلفة من أجهزة الكمبيوتر.

الحصري في هذه الطريقة أنها قادرة على مسح عدونا هذا (الفيروس أو الدودة) من على جهازك حتى لو كان TAZEBAMA.dll وهي دودة بليدة من الصعب القضاء عليها في بعض الاحيان تبقى حتى بعد عملية الفورمات. كما سنتمكن من إسترجاع ما أفزدته في نظامنا... يعني كأنها لم تدخل حاسوبك البتا.

***

1-لنتعرف على TAZEBAMA

*يتسائل البعض لما سنقوم بالتعرف على الـــ TAZEBAMAفقط؟

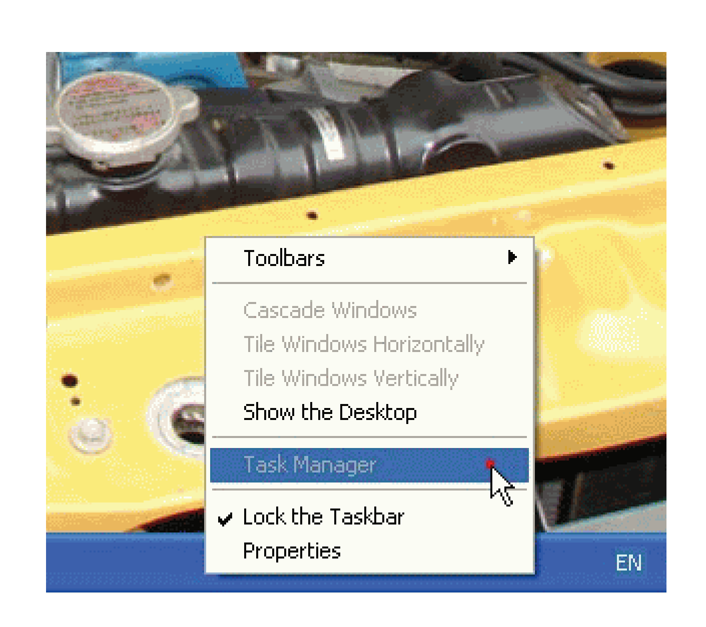
ذلك لأن TAZEBAMAهي من الصعب التخلص عليها ،وحينما تصبح قادرا على التخلص منها ، تصير قادرا على التخلص من أي فيروس أخر .

*كيف يصاب جهازنا بهذه الفيروس؟

أي فيروس قادر على إصابة جهازنا إثر دخوله عبر فلاش ديسك أو قرص ليزري أو عبر الإنترنت. وذلك عندما نحمل ملفات خاصة تحت إمتداد RAR.*أو ZIP.* أو أي ملف مظغوط أخر، من مواقع غير موثوق بها .

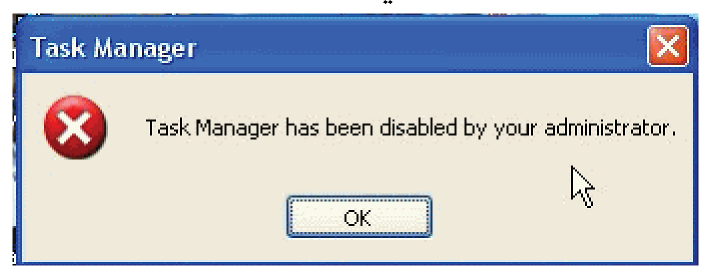
*كيف نتأكد من وجود TAZEBAMAأو فيروس أخر بجهازنا ؟

عندما يصاب جهازنا بفيروس وخاصة الـــــ. TAZEBAMA نصير غير قادرين على فتح Task Manager. كما هو مبين في الصورة 1-1.



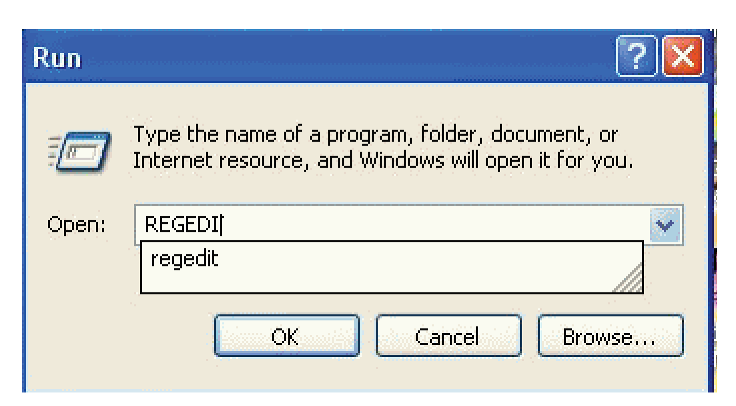
1-1

أو عند الضغط على ctrl+alt+del معا وتظهر لك هذه الرسالة . كما هو مبين في الصورة 1-2.



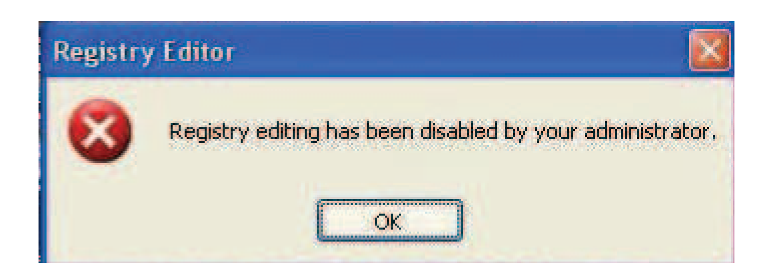
2-1

2- لا يمكنك التعديل على الريجيستري وذلك لعدم قدرتك للدخول إليه . Start>Run ثم تكتب Regedit كما هو مبين في الصورة 1-3.



3-1

فتظهر هذه الرسالة المبينة في الصورة 1-4.



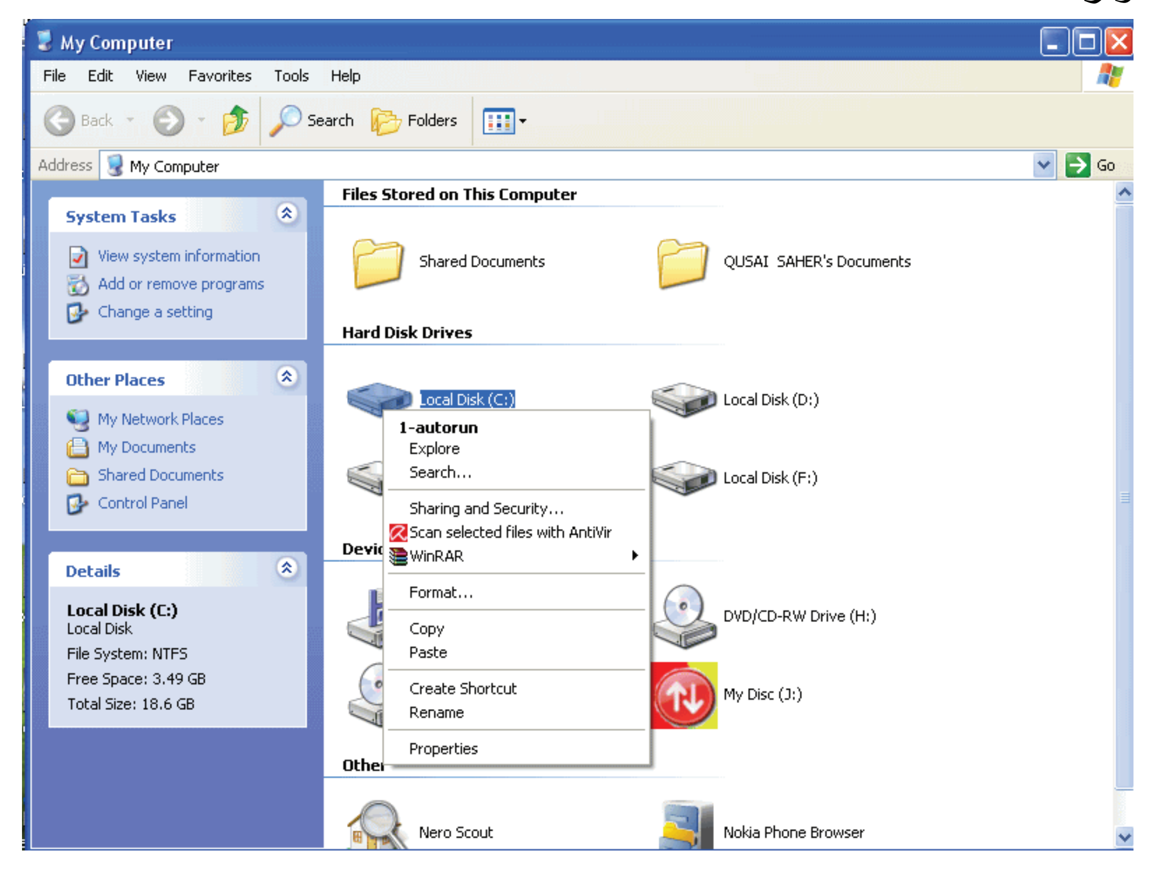
4-1

3- ستلاحظ أنك بمجرد ظغطك على أيقونة القرص الصلب يفتح لك ملف الديسك في نافذة جديد ، إضافة إلى التفطن إلى ثقل في مردود الحاسب خاصة في الأجهزة القديمة .

لنتبع هذه الخطوات لنتأكد أكثر :

أولا: ننقر بالزر الأيمن للفأرة على أي قرص صلب.

نجد السطر الأول يحمل الإسم autorun.inf كما هو مبين بالصورة 5-1.



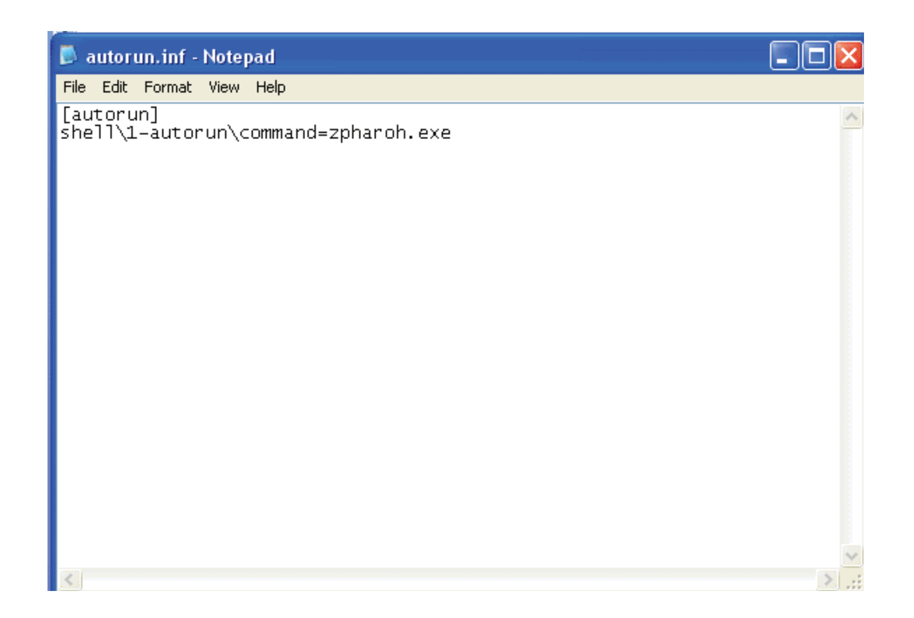
5-1

ثانيا: ننقر على Explorer. سنجد ملف بنفس الإسم autorun.inf ننقر على هذا الاخير بالزر الأيمن للفأرة. ونختار modifier. يفتح لنا الملف من خلال برنامج NotPad. وسنجد به هذه الأسطر مكتوبة:

{autorun}

Shell\1-autorun\command=zpharoh.exe

كما هو مبين بالصورة 6-1.



6-1

إذا هذا الملف المسمى بـ autorun.inf يعمل تلقائيا بمجرد محاولة دخولك للقرص. و عمله يؤتي حتما إلى عمل الفيروس. و الذي لقب هنا بـ zpharoh و هو الـ TAZEBAMA شخصيا .

* * *

2-المرحلة التحضيرية

لا أنصح بحرق هذه المرحلة لأنها تعتبر أساسية في نجاح العملية، حيث انها تمثل 50% منها .

سنقوم في هذه المرحلة بإيعاقة حركة الفيروس. وذلك بإيقافه، لأنه لا يمكن فسخ شيئ من على الحاسوب وهو إثر العلم أو الإشتغال.

إذا تتطرقنا فيما سبق أن الفيروس TAZEBAMA يقوم بتعطيل كل من Task Manager و RegEdit. لذلك سنقوم الان بإعادة تفعيليهما .

أولا: * نذهب Start>Run

* نكتب GPEDIT.MSC ثم Enter

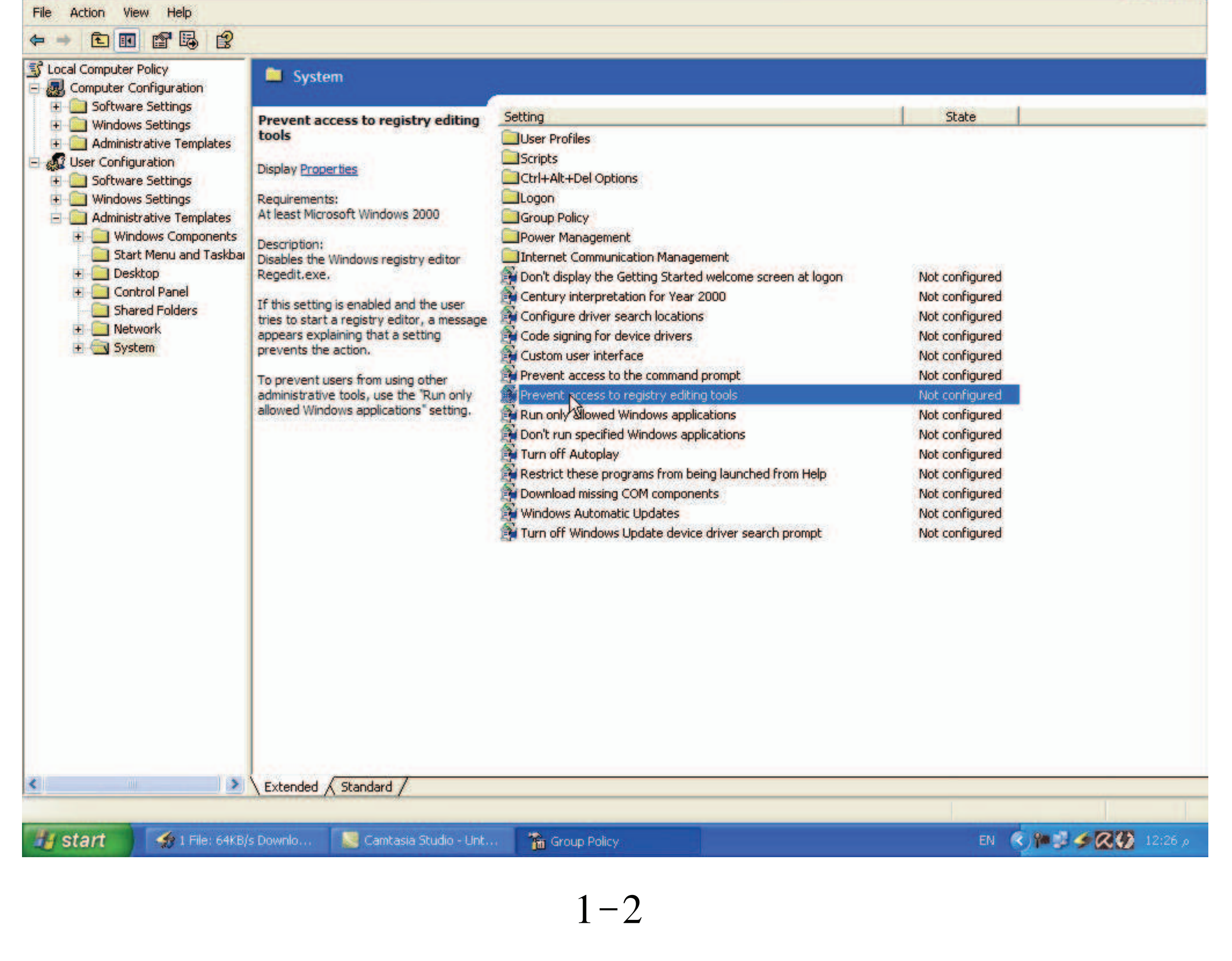
* يظهر لنا كما هو مبين في الصورة 2-1

* ثم نختار

USER CONFIGURATION>ADMINISTRATIVE TEMPLATES >SYSTEM

* ثم نختار منها PREVENT ACCESS TO REGISTRY TOOLS

* إختر من النافذة التي ستضهر لك Disable



1-2

ثانيا : تشغيل Task Manager:

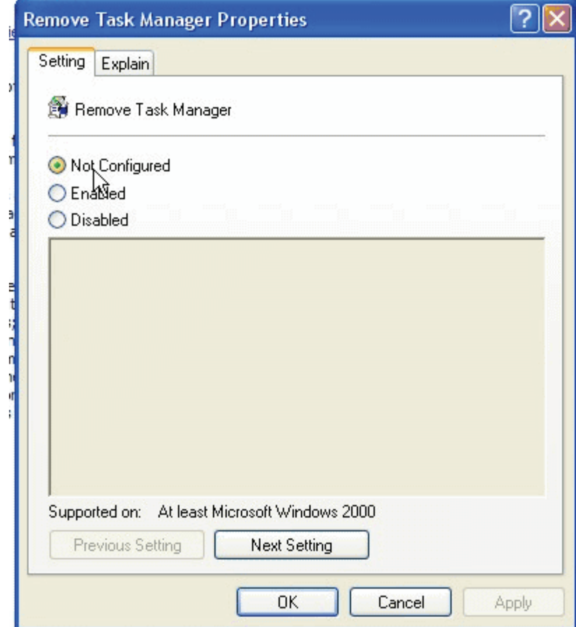
*من نفس الملف System.

*نختار منه الملف ctrl+alt+delOption

*التي نختار منها Remove Task Manger. كما هو مبين بالصورة 2-2.

2-2

*كما فعلنا سابقا نختار Disable. كما هو مبين بالصورة 2-3.



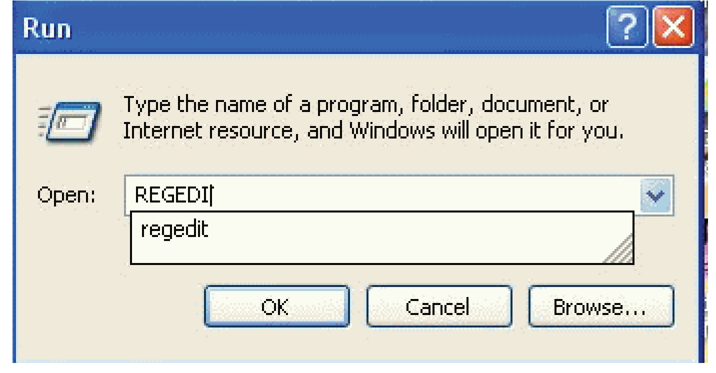
3-2

الأن وبعد تشغيل الـ Task Manager و الـ RegEdit أين تكمن الأهمية ؟

الان يمكننا من خلال RegEdit خذف مفتاح الفيروس من قائمة الـStartUp لكي لا يفتح مجددا بمجرد فتح الجهاز.

كيف نقوم بذلك؟

سهل جدا نفتح RegEdit عن طريق الدخول إلى Start>Run ثم كتابة RegEdit. كما هو مبين في الصورة 4-2.

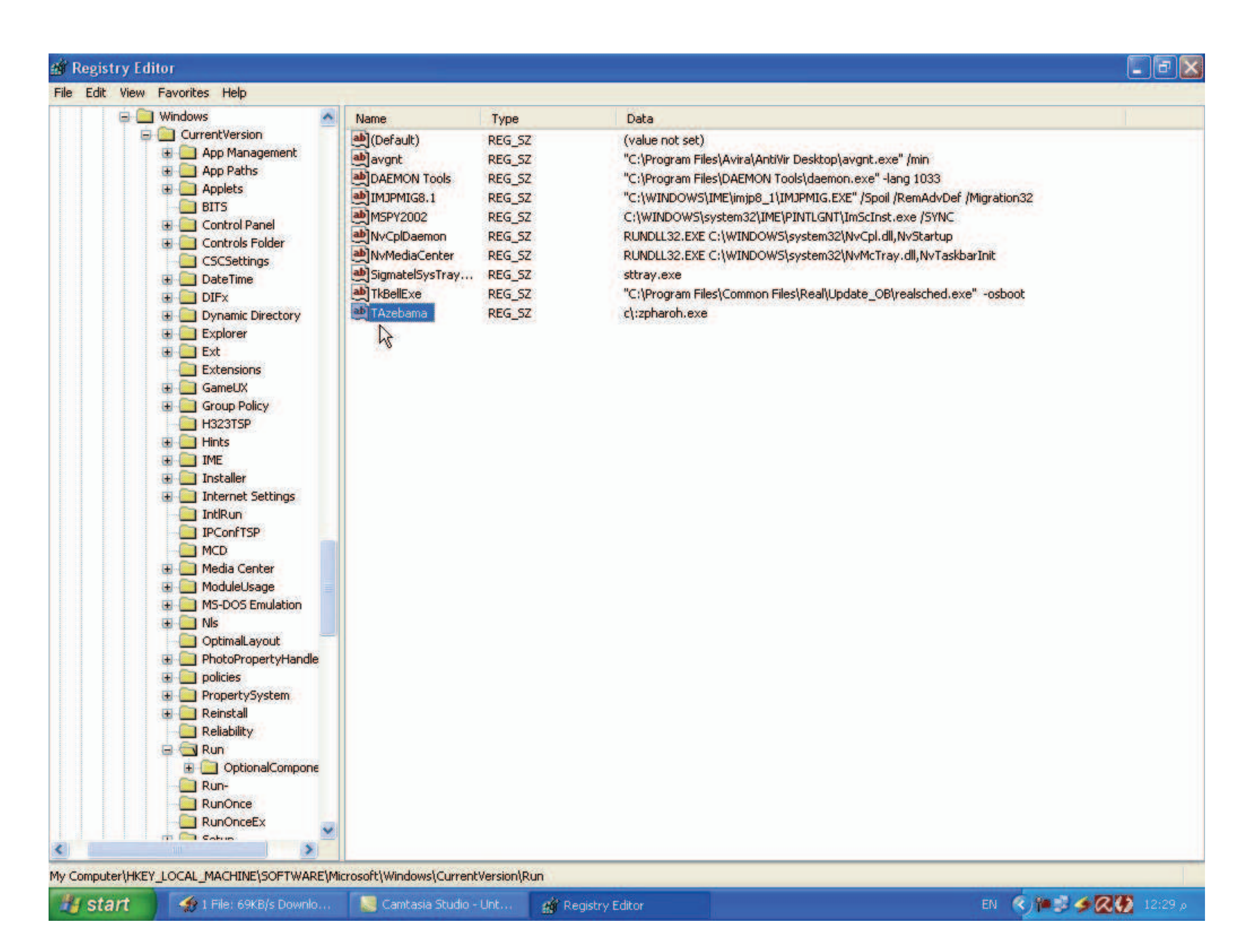


4-2

ثم إتبع

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curr entVersion\Run

كما هو مبين في الصورة 5-2



من تلك القائمة إختر الإسم المشبوه، أنقر عليه بالزر الأيمن للفأرة و إختر Delete.

لدينا هنا zpharo.exe المسمى بـTazebama. نتخلص منه.

الأن نقوم بإعادة تشغيل النظام الخالي من الفيروس وستلاحظ الفرق في سرعة الحاسوب قبل وبعد غلقه...

بعد الأن مازالت مرحلتان مهمتان: تنظيف الكمبيوتر وصيانته.

لإعادة تشغيل الجهاز Start>Shutdow>Restart

* * *

3-مرحلة التنظيف

في الفصل السابق قمنا بإصلاح كل من Task Manager و RegEdit.

إذا الأن لنتأكد من عدم إشتغال ألفيروس مع النظام. لأنك من الممكن أن لا تتفطن إلى فيروس في قائمة الـStarUp.

نظغط ctrl+alt+del ونختار processesونبحث عن إسم مشبوه. في الأغلب لن تجده لكن مجرد تأكد فقط.

لنبدأ الان عملية التنظيف والتي تأخذ الكثير من الوقت.

سنحتاج قبل كل شيئ برنامج Dr.Web للبحث عن الفيروسات وحذفها.

لتحميله نذهب إلى هذا الرابط (البرنامج مجاني وفعال).

http://www.softpedia.com/get/Antivirus/Dr-WEB-CureIt.shtml

كما تلاحظون التحميل سيكون من موقع SoftPedia.com وهو موقع معروف لتحميل البرامج المجانية وهو موثوق به.

عند دخولك للرابط المذكور أعلاه، ستجد الصفحة التي تراها في الصورة 3-1.



1-3

نظغط DOWNLOAD ونقوم بالتحميل و هي عملية سهلة لا تتطلب الشرح.

عند إنتهاء عملية التحميل تتبع الرابط الذي إخترته . وتنقر على أيقونة البرنامج كما هو مبين في الصورة 3-2.



2-3

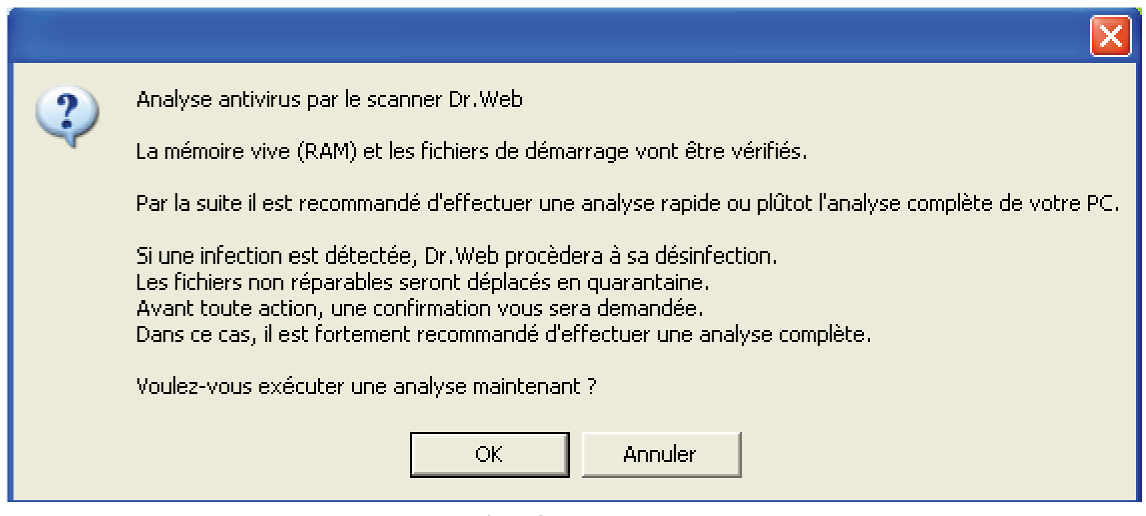
البرنامج لا يحتاج إلى التنصيب.

إذا فبعد الظغط على أيقونة البرنامج ستظهر لنا نافذة كما في الصورة 3-3. نختار منها Commencer le Scan كما هو مبين.



3-3

عند ها تظهر لنا رسالة مثل الموجودة في الصورة 3-4. نختار منها ok.



4-3

تسألنا الرسالة إن كنا نريد فحص الذاكرة Ram وقد أجبناه بنعم.

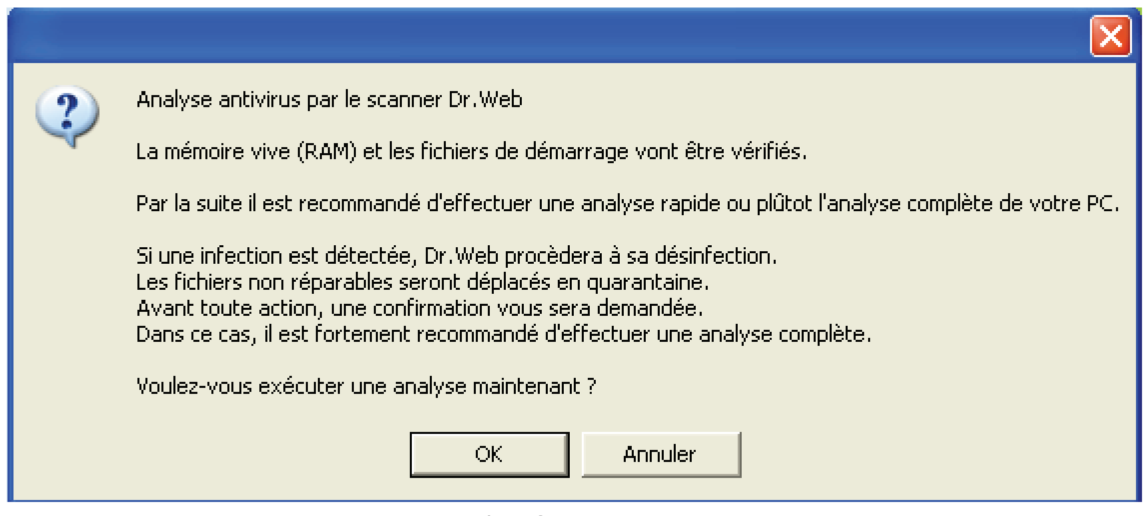
لذلك ستبدأ بالفحص كما هو مبين في الصورة 3-5.

إذا ينبغي إنتظر ها حتى تنتهي.



3-3

عند ها تظهر لنا رسالة مثل الموجودة في الصورة 3-4. نختار منها ok.



4-3

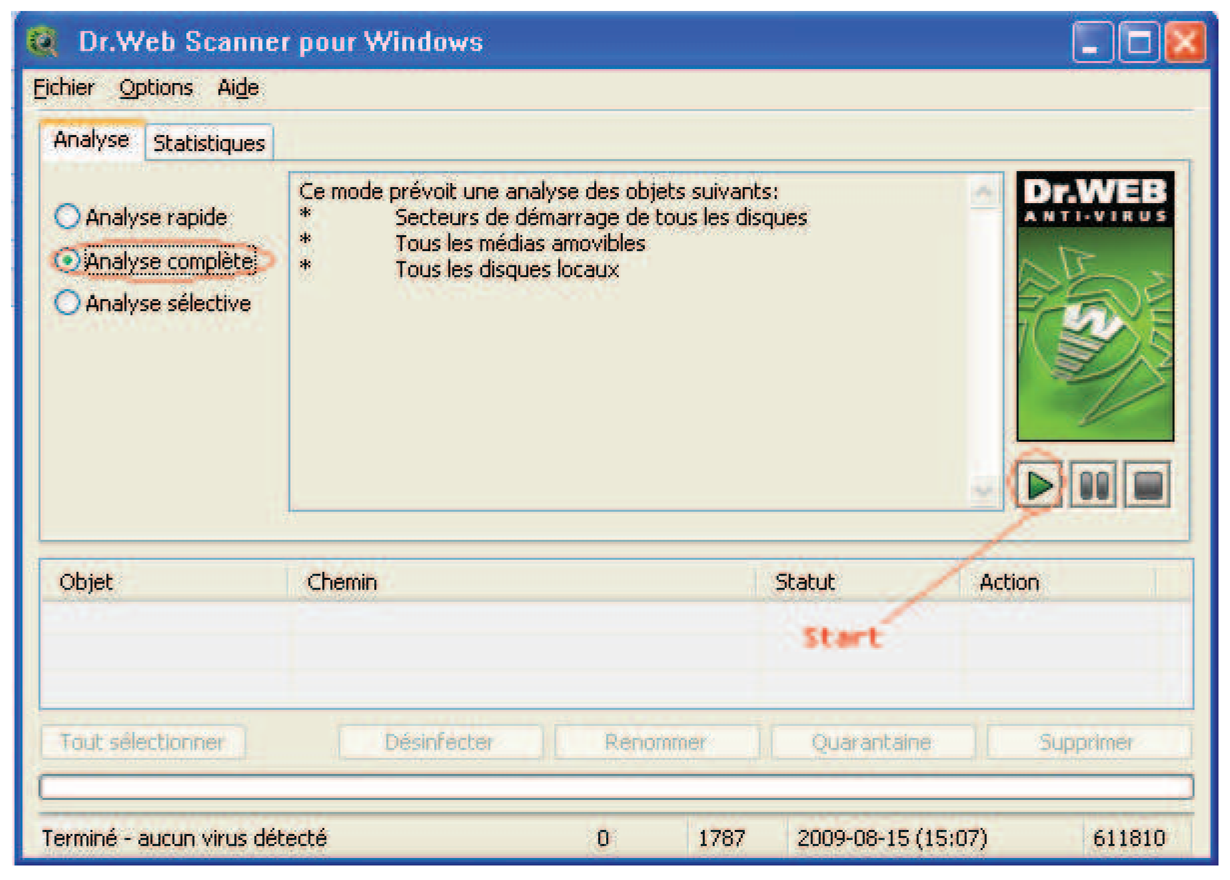
تسألنا الرسالة إن كنا نريد فحص الذاكرة Ram وقد أجبناه بنعم.

لذلك ستبدأ بالفحص كما هو مبين في الصورة 3-5.

إذا ينبغي إنتظرها حتى تنتهي.

5-3

عند الإنتهاء نختار Analyse Complète ثم Start. كما هو مبين في الصورة 6-3.



6-3

حينما يقبض على فيروس سيظهر لك رسالة تسألك فيما إن كنت تريد حذف الفيروس فأجبه بـ yes to all.

وعندما ينتهي من البحث والحذف أغلقه. وقم بإعادة تشغيل النظام.

أما الأن فمازالت الخطوة الأخيرة وهي إعادة النظام إلى حالته الطبيعية.

***

4-مرحلة صيانة النظام

في هذه المرحلة السهلة و المهمة سنحتاج إلى برنامج لأعادة مفاتيح الريجيستر و غيرها إلى حالتها الطبيعية، يعني كأننا قمنا بإعادة تنصيب النظام.

البرنامج مجاني يسمى System Repair Engineer. سنقوم بتحميله من موقع أخر معروف في تحميل البرامج المجانية، و هو موقع أمن.

إذا من هنا نقوم بتحميل البرنامج:

http://download.cnet.com/System-Repair-Engineer-SREng/3000-2094_4-10707166.html?tag=mncol

إثر دخولنا لهذا الرابط سنتحصل على الصفحة المبينة في الصورة 4-1.

System Repair Engineer (SREng) 2.5.16





CNET editors' review

Reviewed by: CNET Staff

It offers a simple way to help users troubleshoot system issues, but the program is best used by experienced-to-expert users. System Repair Engineer's operation is intuitive. That's important since the primary Help file opens an online Simplified Chinese manual. Fortunately, individual functions include short help pop-ups in English.

After a short introduction, users can start tests by clicking on one of the three function buttons. Boot Items opens an eight-tab dialog that lists programs and services loaded at system start-up. Columns are easily sorted with a click. Deleting, adding, or editing start-up items is easily accomplished. The System Repair function presents simple lists of problem file associations, Windows shell options, Browser add-ons, Host file items, and Winsock providers.

Quick specs

Price: Free

Operating system: Windows Vista, Windows Me, Windows XP, Windows 2000, Windows 98

Date added: July 16, 2007

Total Downloads: 22,070

Downloads last week: 122

See full specifications »

1-4

بعد ذلك ننقر على أيقونة Download Now، ونقوم بعملية التحميل و هي سهلة لا تحتاج للشرح.

عند إنتهاء التحميل، تذهب إلى المسار الذي إخترته لتحميل البرنامج. ثم تنقر على أيقونته المبينة بالصورة 2-4.



2-4

ستظهر لنا هذه النافذة الموجودة بالصورة 3-4.

CFF158EE8

Tools Help

About SREng

Boot Items

System Repair

Smart Scan

Extensions

About SREng

System Repair Engineer(SREng) is a tool to adjust, repair your system, and find unknown malwares.

Smallfrogs, who awarded "Microsoft Most Valuable Professional for Windows Shell/User" award in 2004, 2005, 2006, 2007 and 2008 designed this tool.

With the help of this tool, you can detect your system issues and repair them easily.

System Repair Engineer(SREng) is comprised with major base components and basic functions.

The major base components include [Advanced Security Diagnosis] component, [Smart Scan] component, [Plugin/Extension Support] component and so on.

The basic functions include [Windows Boot Items Control], [Service/Driver Control], [File Association Repair], [System Repair] and so on.

As a powerful System Configuration and Security Diagnosis tool, System Repair Engineer(SREng) hope you can share your advice with the author of System Repair Engineer(SREng): Smallfrogs.

You can mail your advices or bugs to support@KZTechs.com, we will help you to solve your question for free.

Welcome to visit the official site of System Repair Engineer(SREng) (http://www.KZTechs.com) for more information.

PayPal DONATE

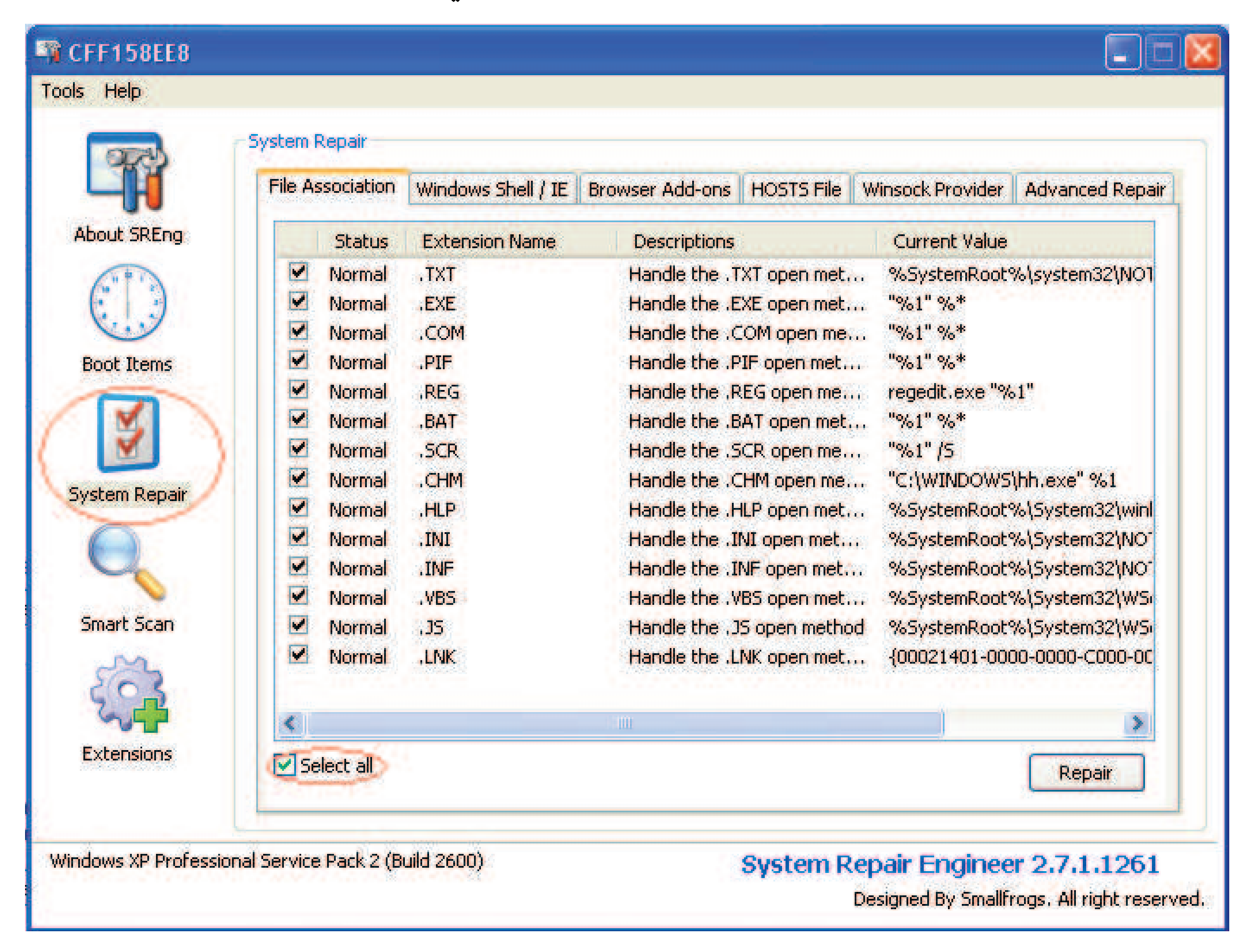
Windows XP Professional Service Pack 2 (Build 2600)

System Repair Engineer 2.7.1.1261

Designed By Smallfrogs. All right reserved.

3-4

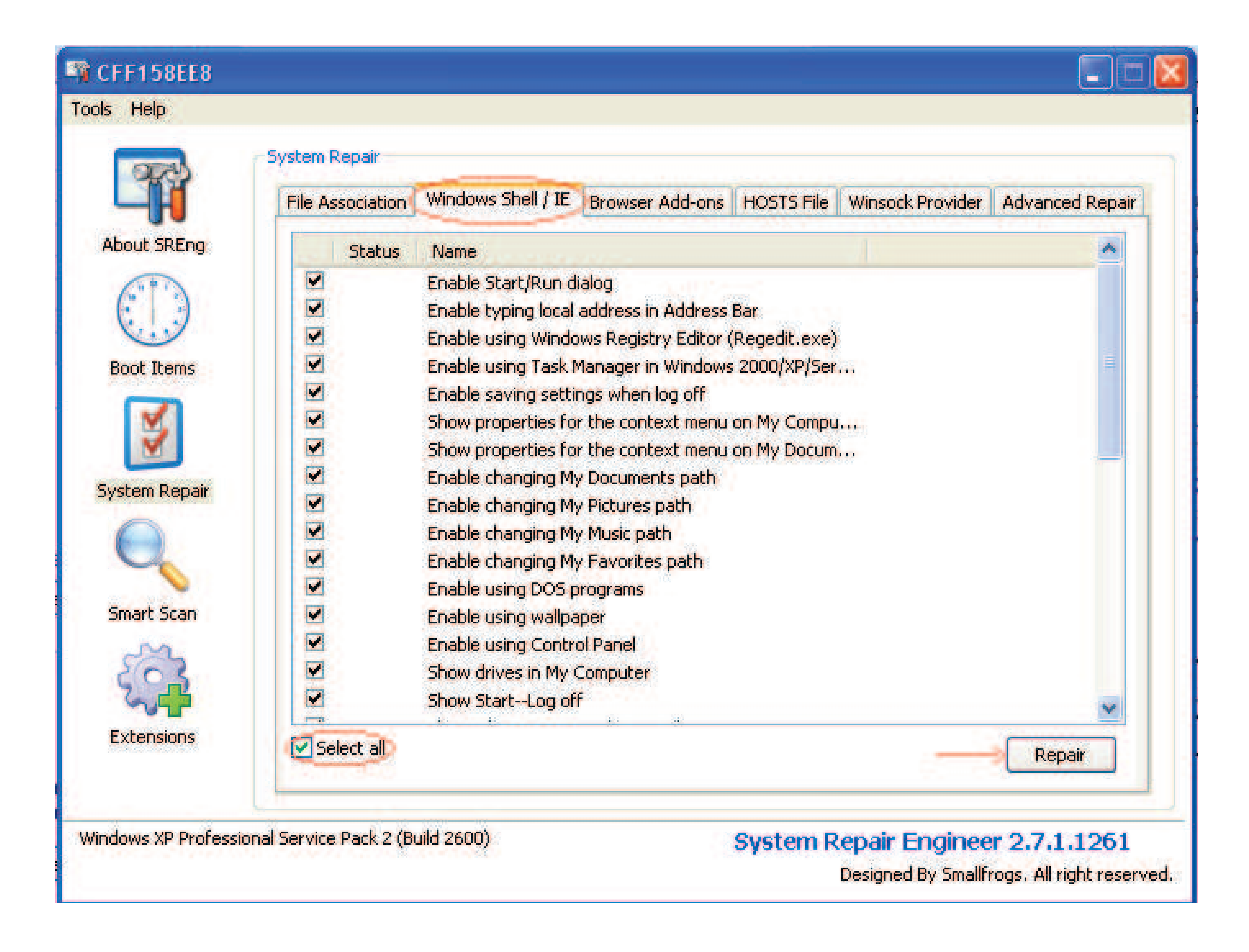
إذا نختار من اليسار System Repair، ومن ثم نختار من الأسفل Select All، كما هو مبين في الصورة 4-4.



4-4

ننقر فيما بعد على Repair.

وبعد الإنتهاء سنختار من الاعلى Windows Shell/IE، ونقوم بنفس العملية كما هو مبين بالصورة 4-5.



5-4

الان نغلق البرنامج ونقوم بإعادة تشغيل نظامنا الخالي من الفيروسات. وستلاحظ كأنك قمت بالفورمات لكنك إحتفظت بملفاتك...

* * *